AF ZKW

PATENT
09/801,614

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	:	Group Art Unit: 2143
	:	Examiner A. M. Lezak
Gerald F. McBrearty et al.	:	Intellectual Property
Serial No: 09/801,614	:	Law Department - 4054
Filed: 03/08/2001	:	International Business
Title: PROTECTING CONTENTS	:	Machines Corporation
OF COMPUTER DATA FILES FROM	:	11400 Burnet Road
SUSPECTED INTRUDERS BY	:	Austin, Texas 78758
PROGRAMMED FILE DESTRUCTION	:	Customer No. 32,329
Date: 10/5/05	:	

CERTIFICATE OF MAILING

I hereby certify that this correspondence including a Brief on Appeal (in triplicate), and this transmittal letter (duplicate) is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450 on 10/5/05.

J. B. KRAFT

Signature J. B. Kraft Date 10/5/05

TRANSMITTAL OF APPELLANTS' BRIEF UNDER 37 CFR 1.192(a)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached is Appellants' Brief (in triplicate) in this Appeal from a decision of the Examiner dated May 5, 2005 finally rejecting claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30.

Please charge our Deposit Account No. 09-0447 in the amount of $500.00 for the Appeal Brief fee. (a duplicate of this transmittal is included.)

The Commissioner is hereby authorized to charge any additional fee which may be required or credit any overpayment to Deposit Account No. 09-0447.

Respectfully submitted

J. B. Kraft 10/5/05

J. B. Kraft
Attorney for Applicants
Registration No. 19,226
(512) 473-2303

PLEASE MAIL ALL CORRESPONDENCE TO:

Herman Rodriguez
IPLaw Dept. - IMAD 4054
IBM Corporation
11400 Burnet Road
Austin, Texas 78758

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	:	Group Art Unit: 2143
	:	Examiner A. M. Lezak
Gerald F. McBrearty et al.	:	Intellectual Property
Serial No: 09/801,614	:	Law Department - 4054
Filed: 03/08/2001	:	International Business
Title: PROTECTING CONTENTS	:	Machines Corporation
OF COMPUTER DATA FILES FROM	:	11400 Burnet Road
SUSPECTED INTRUDERS BY	:	Austin, Texas 78758
PROGRAMMED FILE DESTRUCTION	:	Customer No. 32,329
Date: 10/5/05	:	

BRIEF ON APPEAL

Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal from the Final Rejection of Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 of this Application dated May 5, 2005. Section VIII. Appendix containing a copy of each of the Claims is attached.

I. Real Party in Interest

The real party in interest is International Business Machines Corporation, the assignee of the present Application.

II. Related Appeals and Interferences

None

III. Status of Claims

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

There are 14 claims in this Application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 2, 3, 6, 8, 9, 11, 12, 15, 16, 18, 19, 22, 23, 26, 28, 29.
2. Claims withdrawn from consideration but not cancelled: None.
3. Claims pending: 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30.
4. Claims allowed: None.
5. Claims rejected: 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30.

C. CLAIMS ON APPEAL

Claims on appeal: 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30.

IV Status of Amendments

No amendments have been filed after Final Rejection.

V. Summary of Claimed Invention

The present invention involves the recognition that there are systems having data files so sensitive that the system may be programmed to have the requested files destroyed at the first unauthorized request for access to the file contents. Thus, the invention provides a very aggressive solution to the problem of unauthorized intrusions into database files. It provides for storing for each of the plurality of data files, a backup file which is inaccessible to any user requests. Then, as soon as an initial unauthorized intrusion is determined, the requested data files are destroyed, and the respective stored backup files are substituted for the destroyed files.

Accordingly, the present invention (as defined in independent claims 1, 10, and 21) provides an implementation for protecting the data files from unauthorized users comprising means for storing for each of said plurality of data files, a backup file inaccessible to user requests (Application page 4, lines 3-5);

means for receiving user requests for access to data files (Application, p. 10 lines 22-27 referring to Fig 4, steps 88-90);

means for determining whether said requests are unauthorized intrusions into said requested data files (Application p.10 line 25 through page 11, line 34, referring to steps 93-97, Fig 4.);

means responsive to an initial determination that a request is unauthorized for destroying the requested data files (Application, page 11, lines 7-12, and lines 20-24 referring to Fig. 4 of the drawings); and

means for reloading a backup file for each destroyed file (page 12, lines 1-6, with reference to Fig. 4 of the

drawings).

Independent claims 5, 7, 14, 17, 25, and 27 cover the above described invention in a network environment, e.g., the World Wide Web. Fig. 1 is described in the Specification showing the implementation being carried on the World Wide Web network. (Page 6, lines 1-20).

Dependent claims 4, 13, 20, 24, and 30 cover a further embodiment of the above described general invention wherein an unauthorized intrusion is determined by determining whether a user access identification has been denied (Application, page 11 lines 20-24) and whether the user (intruder) has already copied the requested the requested files (page 11, lines 20-24 referring to Fig. 4.

VI. Grounds of Rejection

Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 are rejected under 35 U.S.C. 103(a) over the combination of Schneck (US5,933,498) in view of Groshon (US6,351,811).

VII. Argument

Claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 are unobvious over the combination of Schneck (US5,933,498) in view of Groshon (US6,351,811), and, thus, are patententable under 35 U.S.C. 103(a).

The Final Rejection of claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 as being unpatentable under 35 U.S.C. 103(a) over the combination of Schneck (US5,933,498) in view of Groshon (US6,351,811) is respectfully traversed.

The present invention involves the recognition that in many systems, the data files may be so sensitive that the system may be programmed to have the requested files de-

stroyed at the first unauthorized request for access to the file contents. Thus, the invention provides a very aggressive solution to the problem. It provides for storing for each of the plurality of data files, a backup file which is inaccessible to any user requests. Then, as soon as an initial unauthorized intrusion is determined, the requested data files are destroyed, and respective stored backup files are substituted for the destroyed files.

The two cited references, neither singly or in combination suggest the specific implementation of the present invention for such data protection.

Schneck et al. (US5,933,498) The Basic Reference

The Examiner admits that Schneck does not teach storing for each of said plurality of data files, a backup file inaccessible to user requests. However, the Examiner has failed to note that Schneck also fails to disclose reloading a backup file for each destroyed file.

Thus, while Schenck has a general concern with whether data found to be corrupted by unauthorized intrusion should be destroyed, the reference fully fails to disclose either of the above elements in Applicants' novel combination solution in response to such an intrusion.

Gorshon et al. (US6,351,811) the Modifying Reference Fails to Make Up for the Deficiencies of the Basic Schneck et al. Patent

The teachings in Groshon fail to make up for these deficiencies in the basic Schneck patent. While the Examiner has pointed to general statements in Groshon related to backup data files, and the additional security offered by such files, Groshon still fails to suggest Applicants' aggressive response to a detected unauthorized intrusion

into a data file: there is stored for each data file, a backup file which is inaccessible to any user requests. Then, as soon as an unauthorized intrusion is initially determined, the requested data file is immediately destroyed, and stored backup file is substituted for the destroyed files.

Actually, the general statements in Groshon could lead one skilled in the art away from making the Examiner's proposed combination of elements. For example, Groshon (at col. 6, lines 34-38) states that there may be circumstances where compromised and suspect data may be transmitted and used. This certainly would lead one skilled in the art away from Applicants' immediate solution of immediate destruction of the intruded data file, and the substitution of the stored backup file.

Combination of Schneck and Groshon has been Made Solely in Light of Applicants' Own Teaching

Applicants submit that the Examiner's combination of Schneck and Groshon references is being made not with the requisite foresight of one skilled in the art, but rather with the hindsight obtained solely by the teaching of the present invention. This approach cannot be used to render Applicants' invention unpatentable. What the Examiner has done is used Applicants' disclosure as a guideline, and the picked and combined elements from each of the Groshon and Schneck references based solely of Applicants' own teaching.

> "To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art references of record convey nor suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher." W. L. Gore, 721 F 2d at 1553, 220 USPQ,

pp. 312-313.

> "One cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention." In re Fine, 5 USPQ 2d 1596 (C.A.F.C.) 1988.

Accordingly, it is submitted that the suggestion for combining Schneck with Groshon in the manner proposed by the Examiner could only come from Applicants' own teaching, and, thus, cannot form any basis for a combination of references.

Furthermore, even if the elements from Schneck and Groshon were to be combined in the manner suggested by Examiner, the combination would still lack significant elements of the combination of the present invention i.e. There is 1) stored for each data file, a backup file which is inaccessible to any user requests. Then, as soon as an 2) unauthorized intrusion is initially determined, the requested data file is immediately destroyed, and stored backup file is substituted for the destroyed files.

Examiner's Argument

The Examiner in responding to the Applicants' argument points to an inaccessible "control copy" of the information in the HTML database (described in Gorshon, at col 3, lines 24-37) so that the information in the database may be compared to the control copy to determine if the information has been compromised. Applicants submit that this control copy is used to determine if data has been compromised by comparison to the data in the data base. Thus, this control copy is not used to determine whether a received request for data files is an unauthorized intrusion as claimed in the present invention. Rather, in Gorshon, the control copy

appears to be used, subsequently, to determine if there has been an integrity compromise of the data in the database. Here again, this interpretation of the teaching of Groshon can only have pertinence if made in the light of Applicants' own teaching which as set forth above can not provide the basis for a rejection based upon a combination of references.

Applicants' Argument on Specific Claims

With respect to independent claims 5, 7, 14, 17, 25, and 27 which cover the above described invention in a network environment, e.g., the World Wide Web, Applicants will concede that both Schneck and Groshon relate to network environments. Accordingly, these claims are submitted to be patentable over the combination of Schneck in view Groshon for all set forth hereinabove for the patentability of independent claims 1, 10, and 21.

With respect to dependent claims 4, 13, 20, 24, and 30, these claims cover a further embodiment of the above described general invention wherein an unauthorized intrusion is determined by determining whether a user access identification has been denied and whether the user (intruder) has already copied the requested the requested files. Of course, these claims are submitted to be patentable over the combination of Schneck in view Groshon for all set forth hereinabove for the patentability of independent claims 1, 10, and 21. In addition, these dependent claims cover a combination of events which would indicate an immediate unauthorized intrusion. While Schneck may disclose the individual elements of rejecting or denying access ID codes or determining whether files have been copied, there is no disclosure in the references of this combination of events triggering a destruction of database

files.

Conclusion

In view of the foregoing, claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 are submitted to be unobvious over the combination of Schneck (US5,933,498) in view of Groshon (US6,351,811) under 35 U.S.C. 103(a) and, thus, are patentable.

Accordingly, the Board of Appeals is respectfully requested to reverse the final rejection and find claims 1, 4, 5, 7, 10, 13, 14, 17, 20, 21, 24, 25, 27, and 30 in condition for allowance.

Respectfully submitted,

J. B. Kraft 10/5/05

J. B. Kraft
Attorney for Applicants
Registration No. 19,226
(512) 473-2303

ALL CORRESPONDENCE SHOULD BE DIRECTED TO:

Herman Rodriguez
IPLaw Dept. - IMAD 4054
IBM Corporation
11400 Burnet Road
Austin, Texas 78758

VIII. Claims Appendix

1. In a data processing operation having stored data in a plurality of data files, a system for protecting said data files from unauthorized users comprising:

means for storing for each of said plurality of data files, a backup file inaccessible to user requests;

means for receiving user requests for access to data files;

means for determining whether said requests are unauthorized intrusions into said requested data files;

means responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

4. The data processing operation system of claim 1 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.

5. In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a system for protecting said network site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests;

means associated with a network site for receiving user requests for access to data files;

means at said network site for determining whether said user requests are unauthorized intrusions into said requested data files;

means at said network site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

7. In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a system for protecting said open Web site data files from unauthorized users comprising:

means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests;

means associated with an open Web site for receiving user requests for access to data files;

means at said open Web site for determining whether said user requests are unauthorized intrusions into said requested data files;

means at said open Web site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

10. In a data processing operation having stored data in a plurality of data files, a method for protecting said data files from unauthorized users comprising:

storing for each of said plurality of data files, a backup file inaccessible to user requests;

receiving user requests for access to data files;

determining whether said requests are unauthorized intrusions into said requested data files;

destroying the requested data files responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

13. The data processing method of claim 10 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

14. In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a method for protecting said network site data files from unauthorized users comprising:

storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests;

receiving user requests for access to data files at a network site;

determining at said network site whether said user requests are unauthorized intrusions into said requested data files;

destroying the requested data files responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

17. In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a method for protecting said open Web site data files from unauthorized users comprising:

storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests;

receiving user requests for access to data files at said open Web site;

determining whether said user requests are unauthorized intrusions into said requested data files at said open Web site;

destroying the requested data files at said open Web site responsive to an initial determination that a request is unauthorized; and

reloading a backup file for each destroyed file.

20. The World Wide Web communication network method of claim 17 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

21. A computer program having code recorded on a computer readable medium for protecting data files from unauthorized users in a data processing operation having stored data in a plurality of data files, said program comprising:

means for storing for each of said plurality of data files, a backup file inaccessible to user requests;

means for receiving user requests for access to data files;

means for determining whether said requests are unauthorized intrusions into said requested data files;

means responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

24. The computer program of claim 21 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.

25. A computer program having code recorded on a computer readable medium for protecting data files from unauthorized users in a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, said program comprising:

means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests;

means associated with a network site for receiving user requests for access to data files;

means at said network site for determining whether said user requests are unauthorized intrusions into said requested data files;

means at said network site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

27. A computer program having code recorded on a computer readable medium for protecting open Web sites in a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, said program comprising:

means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests;

means associated with an open Web site for receiving user requests for access to data files;

means at said open Web site for determining whether said user requests are unauthorized intrusions into said requested data files;

means at said open Web site responsive to an initial determination that a request is unauthorized for destroying the requested data files; and

means for reloading a backup file for each destroyed file.

30. The computer program of claim 27 wherein said means for determining whether said user requests are unauthorized include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.